FTC Says Companies Can Collect Kids' Personal Data, As Long As It's Called "Age Verification"

Dan Frieth

The FTC just told companies they can collect children's personal data without parental consent, as long as it's for "age verification."

That's the practical effect of a policy statement the agency issued this week. Under COPPA, websites collecting data on kids under 13 generally need verifiable parental consent first. The FTC's new statement carves out an exception: gather whatever personal information you need to verify someone's age, and the Commission won't come after you for it.

The agency calls this child protection. The infrastructure it's enabling looks different.

Christopher Mufarrige, director of the FTC's Bureau of Consumer Protection, said "Age verification technologies are some of the most child-protective technologies to emerge in decades," and framed the announcement as a tool for parents.

Reclaim Your Digital Freedom.

Get unfiltered coverage of surveillance, censorship, and the technology threatening your civil liberties.

What the statement actually does is green-light personal data collection from minors, on the theory that knowing someone's age requires knowing who they are first.

The exemption is conditional. To avoid enforcement, sites must delete age verification data "promptly" after use, restrict third-party sharing to vendors with adequate security assurances, post clear notices about what they're collecting, and use methods likely to produce "reasonably accurate" results. These requirements are unverifiable by the people whose data gets collected, and enforced by an agency that just announced it won't enforce.

COPPA supposedly exists precisely because children's personal data is sensitive and companies can't be trusted to protect it without legal pressure.

The FTC's new exemption uses that same sensitive data as the price of admission for age verification, then steps back from enforcement. The agency is weakening the law's protections in order to expand the infrastructure that the law was supposedly designed to regulate.

The breach record makes that contradiction concrete. Discord's disclosure that roughly 70,000 users may have had government IDs exposed through a third-party vendor handling age appeals was a preview of what's to come.

Identity documents collected for age verification are high-value targets stored and processed in systems that, as Tea demonstrated months later, can be left completely unsecured. Collecting more of that data, from more platforms, under softer enforcement, doesn't protect children. It just creates more of the same risk at a greater scale.

That breach is instructive. The IDs weren't collected by Discord as part of general surveillance. They were collected specifically for verification. The FTC's new framework would permit exactly that arrangement while calling it a safeguard.

Policy statements describe how an agency plans to use enforcement discretion, not law. The FTC acknowledged this implicitly by announcing it also intends to review the COPPA Rule itself to formally address age verification. The current statement stays in effect until that review concludes in revised regulations, or until the agency pulls it back.

What gets built in the meantime is the issue. Every site that deploys age verification creates a new pipeline: identity documents, biometric scans, or behavioral profiles flowing to platforms to third-party vendors, all of it operating under standards the FTC won't actively police.